



Removing expired NASH Certificate

What is a NASH Certificate?

NASH stands for “National Authentication Service for Health”. They NASH Public Key Infrastructure (PKI) certificates help your practice to:

- access My Health Records;
- securely share health information using software that meets Secure Message Delivery requirements; and
- access the NASH directory on the Certificates Australia website.

Smart Referrals will use the GP practice NASH certificate as part of authentication to verify the practice. NASH certificates are also used to encrypt and decrypt data.

How long do NASH Certificates last?

NASH PKI certificates expire two years from the date of issue. Before your certificate expires, you need to request a new NASH PKI so you can keep using My Health Record and other applications (such as Smart Referrals) that require these certificates for the secure transmission of data.

Medicare will send you a reminder letter 6 week before your existing one expires. It is important that you work with your local IT support provider to promptly install the new certificate and remove expired certificates.

Why should you remove expired certificates?

It is important to remove old certificates from your practice to:

- Avoid GPs having to manually review and select the current certificate every time they access applications that use these certificates (such as Smart Referrals); and
- To avoid users accidentally selecting the incorrect certificate which would result in technical issues, limiting their ability to use the system.

Who should remove expired certificates?

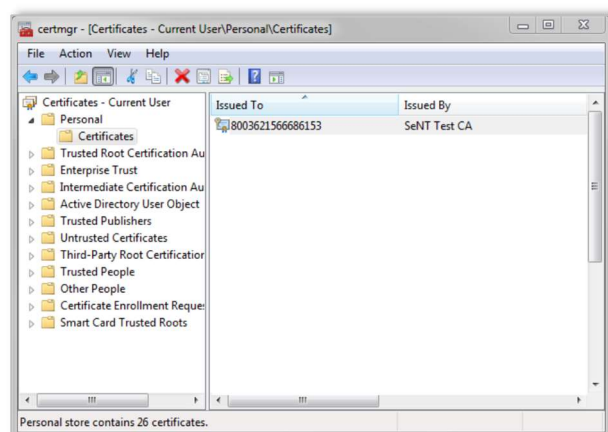
This process is normally undertaken by a General Practice’s local IT Support vendor. Whilst some local IT Support vendors do follow these steps as part of their normal procedures, others do not undertake these steps routinely when installing new certificates, hence it is important to remind them to do this.

IMPORTANT: These instructions should only be undertaken by a skilled IT Technician with appropriate Administration privileges.

How should expired certificates be removed?

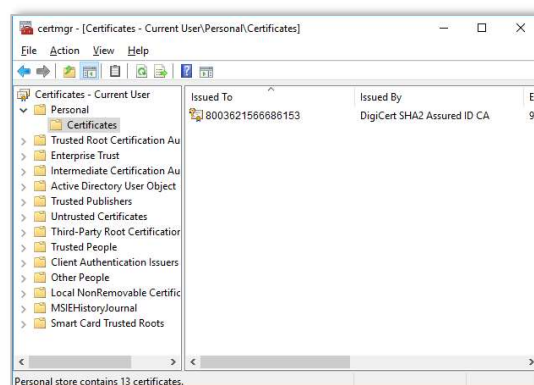
Step 1 – Locate certificates (for Windows 7)

- Select the Start/Windows button and enter “certmgr.msc” in the search box.
- Locate the certificates folder under Personal > Certificates



Step 1 – Locate certificates (for Windows 10)

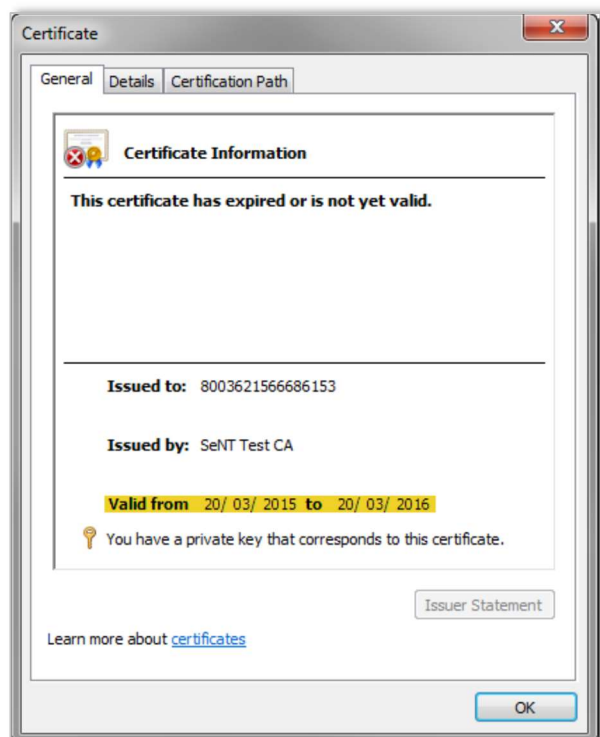
- Select the Start/Windows button and enter “manage user certificates” in the search box.
- Locate the certificates folder under Personal > Certificates



Step 2 – Review NASH Certificate Details

NASH Certificate naming begins with 8003... (sometimes shown as “general.8003”).

- Select the NASH certificate (if available) by double clicking on the certificate
- Check the expiry date (Valid to) to determine if the certificate is current or expired.

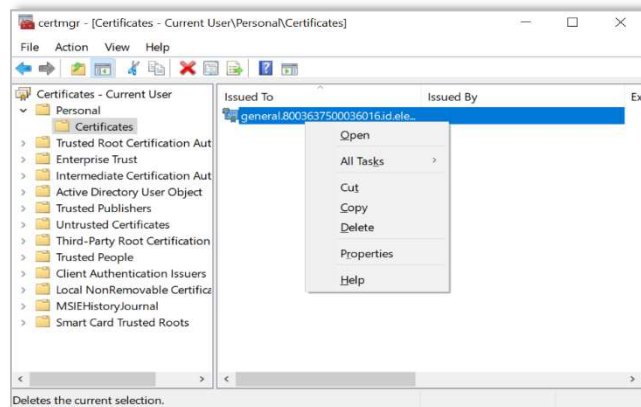


NOTE: Other certificates including Medicare certificates often also coexist in this Personal Store. Please do not open these certificates.

Step 3 – Review expired NASH certificates

Back in the folder, if there are multiple NASH certificates with the same HPI-O number then you will need to delete the older certificate/s with the oldest expiry date/s leaving just the current certificate with a future expiry date.

This is done by highlighting each expired certificate line as demonstrated below and right clicking to bring up options, then left click on “Delete” to remove the older Nash certificate.



IMPORTANT: Please be very careful not to delete any other certificates other than expired NASH certificates (i.e. those without 8003) Medicare certificates often also coexist in this Personal Store.

NOTE: If there are multiple older certificates continue this process until just the current certificate remains.

How to get help

Please contact Smart Referrals Support Team:

Ph: 1300 478 439

Email: CEQ_SmartReferrals@health.qld.gov.au